UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/677,933	10/01/2003	Richard H. Boivie	YOR920030398US1 (8728-647	9603

46069 7590 09/30/2008
F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/677,933
Filing Date: October 01, 2003
Appellant(s): BOIVIE ET AL.

Nathaniel T. Wallace
Reg. 48,909
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/22/2008 appealing from the Office action mailed 2/08/2008.

(1) Real Party of Interest

A statement identifying by name the real party in interest is contained in the brief

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20010050990	Sudia	12-2001
6,185,685	Morgan et al	2-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 11, 14, 16, 18 and 22-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudia (U.S. 2001/0050990).

With respect to calms 11 and 22, a method for ensuring that a processor will execute only authorized code, said method comprising: reading a certificate including a first public key into a protected memory (see paragraph 0249 i.e. the manufacturer could sign a firmware upgrade certificate containing a public key of the third party firmware provider and issue it to that third party... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device); validating said certificate with a second public key permanently stored on said processor (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture); reading a signed authorized code into said protected memory (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto ... upon receiving such an upgrade, the user would load both

the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate); and branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory upon verifying said digital signature (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

With respect to claim 13, wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 14 and 25, wherein said protected memory is physically protected (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 16 and 26, wherein the integrity of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claims 18, wherein the privacy of said authorized code is protected at run time (see paragraph 0248 i.e. tamper-resistant trusted device and paragraph 0249 i.e. sign them with the third party's private signature key).

With respect to claim 23, a computing device for securely executing authorized code, said computing device comprising: a protected memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer) for storing signed authorized code, which contains an original digital signature (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto ... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); and a processor in signal communication with said

protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in of said signed authorized code is original in accordance with first public key stored in said protect memory (see paragraph 0248 i.e. tamper-resistant trusted device that contains an embedded manufacturer's public key, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. The device would then verify the third party's signature on the new code routines against the manufacturer's upgrade certificate and then verify the upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture) and validated by a second public key permanently stored on said processor (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate), and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

With respect to claim 24, wherein the integrity of the contents of said protected memory is protected by encryption (see paragraph 0248 i.e. tamper-resistant trusted device and (see paragraph 0249 i.e. sign them with the third party's private signature key).

Claims 17, 19, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (U.S. 2001/0050990) in view of Morgan et al (U.S. Patent # 6,185,685).

With respect to claims 17 and 27, Sudia does not teach wherein the integrity of said authorized code is protected with symmetric key encryption. Morgan teaches wherein the integrity of said authorized code is protected with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31). Morgan teaches using a symmetric key to encrypt and decrypt the encrypted public key (Ober's encryption algorithm that gets digital signed) (see Morgan column 8 line 60 - column 9 lines 31). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used a symmetric key to encrypt and decrypt the encrypted public key (Ober's encryption algorithm that gets digital signed) to increase the security to the encryption algorithm (see Morgan column 2 lines 32-65). Therefore one would be motivated to have encrypted the authorized code with a symmetric key before storing it in the protected memory and decrypted the authorized code with the symmetric key for execution of the authorized code.

With respect to claims 19 and 28, wherein the privacy of said authorized code is protected at run time with symmetric key encryption (see Morgan column 8 line 60 - column 9 lines 31).

(10) Response to Argument

Applicant's arguments with respect to Sudia not teaching "preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key" in claims 11, 22 and 23 have been considered but are not persuasive.

Sudia dislcoses "preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key" in paragraph 0249 i.e., In an instance of third party upgrade, the manufacturer could sign a firmware upgrade certificate containing a public key (i.e. certificate including a first public key) of the third party firmware (i.e. first public key) provider and issue it to that third party. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key (i.e. signed authorized code), and attach its upgrade certificate (i.e. certificate including a first public key) from the manufacturer thereto. Upon receiving such an upgrade, the user would load both the signed code routines (i.e. signed authorized code) and the manufacturer's upgrade certificate (i.e. certificate including a first public key) into the device and then issue a "process third party firmware upgrade" instruction. The device would then ***verify the third party's signature on the new code routines (i.e. signed authorized code) against the***

manufacturer's upgrade certificate (i.e. certificate including a first public key) and then verify the upgrade certificate (i.e. certificate including a first public key) against the manufacturer's public signature key (i.e. second public key) that was embedded in the device during manufacture. If both signatures verify, the upgrade is accepted and the device performs the desired upgrade.

The Appellant's arguments do not correspond to how the prior art reference was mapped to the claim limitations in the final office action. According to the final office rejection, the Certificate was mapped to the firmware upgrade certificate containing a public key of the third party firmware provider. The First public key was mapped to the public key of the third party firmware provider. The Second public key was mapped to the manufacturer's public key. The Signed authorized code was mapped to the new code routines.

This meets the limitation of the claim language. Reading a certificate including a first public key (i.e. ***public key of the third party***) into a protected memory (see paragraph 0249 i.e. the manufacturer could sign a ***firmware upgrade certificate containing a public key of the third party*** firmware provider and issue it to that third party... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device); validating said certificate with a second public key (i.e. ***manufacturer's public key***) permanently stored on said processor (see paragraph 0248 i.e. tamper-resistant trusted device that contains an ***embedded manufacturer's public key***, a protected non-volatile memory area and a secure central processor unit (CPU) and can upgrade or supplement in a

trusted manner any firmware routines embedded by the manufacturer and paragraph 0249 i.e. verify the ***upgrade certificate against the manufacturer's public signature key that was embedded in the device during manufacture***); reading a signed authorized code into said protected memory (see paragraph 0249 i.e. The third party could then develop, test, and approve replacement or additional firmware routines, sign them with the third party's private signature key, and attach its upgrade certificate from the manufacturer thereto ... upon receiving such an upgrade, the user would load both the signed code routines and the manufacturer's upgrade certificate into the device), wherein said protected memory is cryptographically protected (see paragraph 0249 digital signed data is a type of cryptographically protected data); preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key (see paragraph 0249 i.e. verify the third party's signature on the new code routines against the manufacturer's upgrade certificate); and branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory upon verifying said digital signature (see paragraph 0248 i.e. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature, which signature assures the device that the new firmware code has been developed, tested and approved by the manufacturer and that the device should therefore either (a) overlay one or more currently embedded firmware

routines with the new firmware code or (b) add the new firmware code as one or more new routines in a currently unused area of protected memory).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Devin Almeida/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132